IN THE CLAIMS:

Please cancel claims 1 – 13 in their entirety and without prejudice and substitute the following new claims:

--14. A method for verifying a signature, or respectively an authentication, utilizing an asymmetric private-key and public-key cryptographic calculation process between a "*prover*" entity and a "*verifier*" entity, wherein the prover entity performs first cryptographic calculations with said private key to produce a signature calculation, or respectively an authentication value constituting a response value, and the verifier entity, based on said response value, performs second cryptographic calculations with said public key to perform said signature verification, or respectively said authentication, the first and second cryptographic calculations serving to implement the calculation of modulo-n or large-number multiplications, characterized in that for a cryptographic calculation process using a public key comprising a public exponent e and a public modulo n, and a private key comprising a private exponent, it comprises the following steps"

- calculating at the level of said prover entity at least one prevalidation value;

- transmitting from the prover entity to the verifier entity at least said one prevalidation value, and utilizing said prevalidation value by the verifier entity to perform at least one modular reduction without any division operation for said modular reduction.

15. A method according to claim 14, characterized in that for a public exponent e=2, and wherein the cryptographic calculation process is based on a RABIN algorithm, said at least one prevalidation value comprises a unique value, which is the quotient Q of the square of said respective value of a signature or a response by said public modulo n, Q = R*R/n, where R designates said respective value of a signature or a response to an authentication.

16. A method according to claim 15, characterized in that after the reception by said entity of said respective value of a response to an authentication verification or a signature of a message (M), and of said at least

one prevalidation value comprising said quotient, said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference (D_{AR}, D_{SR}) between the square of the response value R*R and the product Q*n of said quotient Q by said public modulo n, (D_{AR}, D_{SR} = R*R =Q*n; and
- verifying the equality of said difference with the value of a function of said response value, without any division operation by the modulo n operation.

17. A method according to claim 14, characterized in that for a public exponent e = 3, and wherein the cryptographic calculation process is based on an RSA algorithm, said at least one prevalidation value comprises:

- a first quotient Q_1 of the square R*R of said response value R by said public modulo n; and
- a second quotient Q_2 of the product of said response value and the difference between the square R*R of said response value and the product of said first quotient Q_1 and the public modulo n, by said public modulo n, Q_2 = $R*(R*R - Q_1*n)/n$.

18. A method according to claim 17, characterized in that after the reception of said response value R and said at least one prevalidation value comprising said first and second quotients Q_1 and Q_2, said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference (D_{ARSA}, D_{SRSA}) between the product of said response value R and the difference between the square R*R of this response value and the product of said first quotient Q_1 and the public modulo n, and the product of said second quotient Q_2 and said public modulo n (D_{ARSA}, D_{SRSA}) = $R*(R*R - Q_1*n)-Q_2*n$; and
- verifying the equality of this difference with the value of a function of said response value, without any division operation by modulo n operation.

19. A method according to claim 16, characterized in that for an operation for verifying a signature of a message (M), said function comprising a standardized public function f(M) of said message M, said method comprises the following steps:

- applying a condensation function to said message to obtain a message digest CM; and
- concatenating said message digest with a constant value.

20. A method according to claim 18, characterized in that for an operation for verifying a signature of a message (M), said function comprising a standardized public function f(M) of said message M, said method comprises the following steps:

- applying a condensation function to said message to obtain a message digest CM; and
- concatenating said message digest with a constant value.

21. A method according to claim 16, characterized in that, for an authentication verification operation, said method further comprises the step for transmitting a prompt value from the verifier entity to the prover entity.

22. A method according to claim 18, characterized in that, for an authentication verification operation, said method further comprises the step for transmitting a prompt value from the verifier entity to the prover entity.

23. A method according to claim 21, characterized in that said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value A.

24. A method according to claim 22, characterized in that said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value A.

25. A method according to claim 16, characterized in that said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

26. A method according to claim 21, characterized in that said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

27. A method according to claim 22, characterized in that said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

28. A method according to claim 25, characterized in that at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A $\geq$ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of -C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction.

29. A method according to claim 26, characterized in that at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises calculation of the value C*A and storing of said value if C*A < n, and the

calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of -C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction.

30. A method according to claim 27, characterized in that at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of -C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction.

31. A method according to claim 23, characterized in that said function f(A) of said random value A is the function f(A) = A, which makes it possible to verify the equality of said difference and the validity of said authentication without any division operation for the modular reduction.

32. A method according to claim 24, characterized in that said function f(A) of said random value A is the function f(A) = A, which makes it possible to verify the equality of said difference and the validity of said authentication without any division operation for the modular reduction.

33. A method according to claim 14, characterized in that said response value, an encrypted value B, and a quotient value Q are concatenated prior to transmission of the values from the prover entity to the verifier entity.

a6 cont

34. A method according to claim 14, wherein the verifier entity compression embedded system such as a microprocessor card and the prover entity comprises an embedded card reading system.--